UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I“
Centrul de Studii Strategice de Apărare şi Securitate

Dr. Grigore ALEXANDRESCU   Dr. Gheorghe VĂDUVA

INFRASTRUCTURI CRITICE. PERICOLE, AMENINȚĂRI LA ADRESA ACESTORA. SISTEME DE PROTECȚIE

Editura Universității Naționale de Apărare „Carol I”
Bucureşti, 2006

Descrierea CIP a Bibliotecii Naționale a României
ALEXANDRESCU, GRIGORE
Infrastructuri critice: Pericole, amenințări la adresa acestora: Sisteme de protecție /dr. Grigore Alexandrescu, dr. Gheorghe Văduva.- Bucureşti: Editura Universității Naționale de Apărare „Carol I”, 2006
ISBN (10) 973-663-412-4; ISBN (13) 978-973-663-412-3

I. Văduva, Gheorghe

355:327.36

- Lucrarea a fost discutată în şedința Consiliului Ştiințific al CSSAS
- Responsabilitatea privind conținutul revine în totalitate autorilor

ISBN (10) 973-663-412-4;
ISBN (13) 978-973-663-412-3

CUPRINS

ARGUMENT

Infrastructurile critice au reprezentat totdeauna domeniul cel mai sensibil, cel mai vulnerabil al oricărui sistem şi al oricărui proces. Sensibilitatea decurge din rolul lor deosebit în structura, stabilitatea şi funcţionarea unui sistem, oricărui sistem şi oricărui proces. Vulnerabilitatea se defineşte pe imposibilitatea asigurării, prin proiect şi prin realizarea efectivă, a protecţiei corespunzătoare lor, dar şi prin creşterea presiunilor programate, direct sau indirect, intenţionate sau aleatorii asupra lor. Vulnerabilitatea este, în acest caz, direct proporţională cu rolul pe care îl joacă infrastructurile respective. De unde rezultă că, oricât de bine ar fi protejate, infrastructurile critice vor avea totdeauna un grad de vulnerabilitate ridicat, întrucât, de regulă, sunt primele vizate atunci când se urmăreşte destabilizarea şi chiar distrugerea unui sistem sau unui proces. Identificarea, optimizarea şi securizarea infrastructurilor critice reprezintă o prioritatea indiscutabilă, atât pentru gestionarii de sisteme şi procese, cât şi pentru adversarii acestora, adică pentru cei care urmăresc să atace, să destabilizeze şi să distrugă sistemele şi procesele vizate. Infrastructurile critice nu sunt şi nu devin critice, doar la atacuri sau din cauza atacurilor, ci şi din alte cauze, unele dintre ele greu de depistat şi de analizat. De regulă, mai ales după atacurile teroriste de la 11 septembrie 2001 asupra complexului World Trade Center şi asupra Pentagonului, se consideră că infrastructurile sunt sau pot deveni critice în raport cu atacurile teroriste sau cu alte ameninţări, îndeosebi asimetrice. Acesta este doar un aspect sau un criteriu de identificare a infrastructurilor critice. Mai sunt însă şi altele care ţin, deopotrivă, atât de stabilitatea şi funcţionalitatea sistemelor şi proceselor, cât şi de raporturile acestora cu mediul exterior. De aceea, în opinia noastră, analiza problematicii infrastructurilor critice trebuie să ţină seama de toate dimensiunile şi implicaţiile stabilităţii şi funcţionalităţii sistemelor şi proceselor, precum şi de înlănţuirile cauzale care pot genera sau influenţa dinamica lor.

CAPITOLUL 1
DELIMITĂRI CONCEPTUALE

Infrastructurile fac parte din structura de rezistenţă a unui sistem, sunt relaţionale şi funcţionale şi constituie *in integrum* suportul necesar pentru ca sistemul să se identifice, să se individualizeze, să intre în relaţii cu alte sisteme, să se stabilizeze şi, evident, să funcţioneze. Infrastructurile se pot împărţi, în funcţie de locul, rolul şi importanţa lor pentru stabilitatea şi funcţionalitatea sistemelor, precum şi pentru siguranţa şi securitatea sistemelor şi procese în trei mari categorii:

- infrastructuri obişnuite;
- infrastructuri speciale;
- infrastructuri critice.

Infrastructurile obişnuite reprezintă o structură, un cadru, care asigură construcţia şi funcţionarea sistemului. Aceste infrastructuri nu prezintă calităţi deosebite, în afara celor care le justifică existenţa şi prezenţa în cadrul sistemelor şi proceselor. O ţară, spre exemplu, va avea totdeauna drumuri, căi ferate, localităţi, şcoli, biblioteci etc. Pe parcurs, unele dintre acestea pot deveni speciale sau chiar critice, în funcţie de noul rol pe care îl pot avea, de dinamica importanţei şi de alte criterii. Spre exemplu, localităţile care au aerodromuri, puternice centre de comunicaţii, centrale nucleare, noduri de cale ferată etc. pot face parte din infrastructuri speciale şi, în anumite condiţii, chiar din infrastructurile critice.

Infrastructurile speciale au un rol deosebit în funcţionarea sistemelor şi proceselor, asigurându-le acestora o eficienţă sporită, calitate, confort, performanţă. De regulă, infrastructurile speciale sunt infrastructuri de performanţă. Unele dintre acestea, mai ales cele care pot avea, prin extensie sau prin transformare (modernizare), un rol important în stabilitatea şi securitatea sistemelor, pot intra şi în categoria infrastructurilor critice.

Infrastructurile critice sunt, de regulă, acele infrastructuri de care depind stabilitatea, siguranţa şi securitatea sistemelor şi proceselor. Ele pot face parte din categoria infrastructurilor speciale. Nu este însă obligatoriu ca toate infrastructurile care sunt sau pot deveni, la un moment dat, critice să facă parte din această categorie de infrastructuri. Este foarte posibil ca, în funcţie de situaţie, chiar şi unele dintre infrastructurile obişnuite – cum ar fi, spre exemplu, drumurile de ţară sau canalele magistrale din sistemele de irigaţii etc. – să devină infrastructuri critice. De aceea, în definirea infrastructurilor critice, de care ne ocupăm aici, pot să intervină şi alte elemente, ceea ce conduce la concluzia că există un criteriu de flexibilitate şi un altul de imprevizibil în identificarea şi evaluarea unor astfel de structuri.

Infrastructurile critice sunt acele infrastructuri cu rol important în asigurarea securităţii în funcţionarea sistemelor şi în derularea proceselor economice, sociale, politice, informaţionale şi militare.

Infrastructurile sunt considerate critice datorită:

- condiţiei de unicat în cadrul infrastructurilor unui sistem sau proces;
- importanţei vitale pe care o au, ca suport material sau virtual (de reţea), în funcţionarea sistemelor şi în derularea proceselor economice, sociale, politice, informaţionale, militare etc.;
- rolului important, de neînlocuit, pe care îl îndeplinesc în stabilitatea, fiabilitatea, siguranţa, funcţionalitatea şi, mai ales, în securitatea sistemelor;
- vulnerabilităţii sporite la ameninţările directe, precum şi la cele care vizează sistemele din care fac parte;
- sensibilităţii deosebite la variaţia condiţiilor şi, mai ales, la schimbări bruşte ale situaţiei.

Acest tip de infrastructuri există pretutindeni în lume şi, desigur, în fiecare ţară în parte şi în cadrul fiecărui sistem fizic sau virtual, în toate domeniile activităţii omeneşti.

Ele nu sunt stabilite în mod arbitrar, ci doar identificate şi evaluate ca fiind critice. Cu alte cuvinte, din mulţimea de infrastructuri care fac parte dintr-un sistem sau contribuie la funcţionarea unui sistem (proces), numai unele sunt critice. Care dintre ele? Aici intervine un proces de identificare şi evaluare. Criteriile după care se face o astfel de evaluare sunt variabile, chiar dacă sfera lor de cuprindere poate rămâne aceeaşi. Printre aceste criterii, considerăm că s-ar putea situa şi următoarele:

- criteriul fizic, sau criteriul prezenţei (locul în rândul celorlalte infrastructuri, mărimea, dispersia, anduranţa, fiabilitatea etc.);
- criteriul funcţional, sau criteriul rolului (ce anume „face“ infrastructura respectivă);
- criteriul de securitate (care este rolul ei în siguranţa şi securitatea sistemului);
- criteriul de flexibilitate (care arată că există o anumită dinamică şi o anumită flexibilitate, în ceea ce priveşte structurile critice, unele dintre cele obişnuite transformându-se, în anumite condiţii, în infrastructuri critice şi invers);
- criteriul de imprevizibilitate (care arată că unele dintre infrastructurile obişnuite pot fi sau deveni, pe neaşteptate, infrastructuri critice.

Infrastructurile sunt critice, speciale sau obişnuite, în raport cu provocările, pericolele, ameninţările şi riscurile aferente (asumate, impuse sau arondate), dar şi cu determinările şi parametrii de stabilitate, de dinamică şi de funcţionalitate a respectivului sistem sau proces.

De regulă, fiecare sistem şi fiecare proces dinamic sau dinamic complex îşi au propriile lor infrastructuri şi structuri critice. *Structurile critice* ţin de sporirea semnificativă a

sensibilității și vulnerabilităților la pericole și amenințări a relațiilor interioare între elementele de sistem. *Infrastructurile critice* au cel puțin trei componente ale fazelor critice:

- componenta interioară, care se definește pe creșterea (directă sau impusă) a vulnerabilităților infrastructurilor cu rol important în funcționarea și securitatea sistemului;
- componenta exterioară, care se definește pe infrastructurile exterioare cu rol important în stabilitatea și funcționalitatea sistemului și a sistemelor în care sistemul respectiv este integrat, asociat sau relaționat;
- componenta de interfață definită pe mulțimea infrastructurilor din imediata vecinătate, care nu aparțin nemijlocit sistemului, dar îi asigură acestuia relaționările de care are nevoie pentru stabilitate, funcționalitate și securitate.

Deși de infrastructuri critice se vorbește îndeosebi după atacurile teroriste de la 11 septembrie 2001 din Statele Unite, asemenea infrastructuri există de când lumea. Dintotdeauna sistemele – îndeosebi sistemele dinamice complexe și procesele asociate acestora – au avut, în funcționarea și în evoluția lor, momente sau perioade dificile, definite pe o mulțime de perturbații, disfuncționalități, pericole și amenințări, unele dintre acestea fiind asociate unor infrastructuri sau rezultând din inflexibilitatea, inconsistența sau fragilitatea exagerată a acestora.

1.1. Evoluția conceptului de infrastructură critică

Înmulțirea, fără precedent, în ultimele decenii, a riscurilor, pericolelor și amenințărilor la adresa obiectivelor vitale ale statelor și ale organismelor internaționale, concomitent cu creșterea numărului și vulnerabilității acestora, a condus la sedimentarea și statuarea unui nou concept, denumit generic: *infrastructură critică*.

Dacă primele studii în domeniu au identificat obiectivele considerate „critice”, încă din anii ’80, sintagma „infrastructură critică” a fost folosită, în mod oficial, în iulie 1996, când președintele SUA a decretat „Ordinul Executiv pentru Protecția Infrastructurilor Critice”[1]. În preambulul la acest act normativ se explică noțiunea de infrastructura critică drept acea „*parte din infrastructura națională care este atât de vitală încât distrugerea sau punerea ei în incapacitate de funcționare pot să diminueze grav apărarea sau economia SUA*”. Se considera că aceasta cuprindea: telecomunicațiile, sistemul de aprovizionare cu electricitate și apă, depozitele de gaze și petrol, finanțele și băncile, serviciile de urgență (medicală, poliție și pompieri), precum și continuitatea guvernării.

În toamna aceluiași an, a fost înființată Comisia Prezidențială pentru Protecția Infrastructurilor Critice, care a apreciat că securitatea, economia, și chiar supraviețuirea lumii industrializate depind de trei elemente interrelaționate: energia electrică, comunicațiile și computerele[2].

11 septembrie 2001 avea să demonstreze că o țară, oricât de puternică ar fi, nu poate să-și asigure, de una sigură, apărarea eficientă a tuturor centrilor săi vitali. După dezastrul rămas în urma loviturii teroriste, SUA au decis să unească în jurul lor statele lumii care doreau să lupte împotriva acestui flagel.

Globalizarea, odată cu avantajele și transformările pozitive ce le aduce la nivel național, dă posibilitatea propagării rapide, la scară planetară, a amenințărilor directe la adresa securității tuturor. La incercările de globalizare a insecurității trebuia să se răspundă prin măsuri ferme de blocare și eliminare a amenințărilor prezente și pericolelor viitoare și instituirea unui sistem de globalizare a securității.

---

[1] *Executive Order Critical Infrastructure Protection*, http://www.fas.org/irp/offdocs/eo1301htm

[2] http://en.wikipedia.org/wiki/Critical_Infrastructure_Protection

În acest sens, un prim pas a fost făcut de Washington în direcția eliminării vulnerabilității obiectivelor naționale vitale, pe care le preciza ca fiind cele de natură *umană, economică, informațională, din cadrul serviciilor guvernamentale principale și a securității naționale* a SUA. Pentru aceasta, în luna octombrie a aceluiași an, Casa Albă a elaborat: Ordinul Executiv pentru Protecția Infrastructurilor Critice[3]. Prin acesta se urmărea asigurarea continuității conducerii vieții politico-economice și protejarea populației de orice întrerupere a ei[4].

Tema a fost dezvoltată, în 2003, în cadrul Strategiei Naționale de Securizare a Spațiului Cibernetic. Documentul a definit, de data acesta, o compunere a infrastucturii critice mult mai amplă și mai precisă. Astfel, infrastucturile critice reprezentau: „*instituții publice și private din sectoarele agriculturii, alimentației, aprovizionării cu apă, sănătății publice, serviciilor de urgență, guvernării, industriei de apărare, informațiilor și telecomunicațiilor, energiei, transporturilor, bancare și financiare, chimice și a materialelor periculoase, precum și cele poștale și de navigație*"[5].

Nevoia de a defini și proteja în mod organizat centrii vitali ai unei entități a fost resimțită și de organizațiile internaționale. Astfel, în cadrul Alianței Nord-Atlantice, prin infrastructură critică statele membre înteleg: „*facilități, servicii și sisteme informatice care sunt atât de vitale pentru națiuni, încât scoaterea lor din funcțiune sau distrugerea lor poate avea efecte de destabilizare a securității naționale, economiei naționale, stării de sănătate a populației și asupra funcționării eficiente a guvernului*"[6].

---

[3] http://www.whitehouse.gov/news/releases/2001/10/ 20011016-12.html
[4] Idem.
[5] *The National Strategy to Secure Cyberspace, february 2003*, pag. VII.
[6] Apud Dediu George, *Protecți infrastructurilor critice – o nouă provocare*, p.2

În ultimii ani, statele Uniunii Europene au întreprins acțiuni viguroase în direcția stabilirii uni limbaj și unui mod de acțiune comun în vederea protejării obiectivelor lor de valoare strategică. În general, statele comunitare au stabilit în categoria obiectivelor critice: *telecomunicațiile, sursele de apă și de energie, rețelele de distribuție, producția și distribuire a hranei, instituțiile de sănătate, sistemele de transport, serviciile financiar-bancare, instituțiile de apărare și ordine publică (armata, jandarmeria și poliția.* Austria, Franța, Marea Britanie, Spania au înființat organisme specifice, au dezvoltat metodologii, și au alocat fonduri substanțiale pentru protecția infrastructurilor desemnate drept critice. Germania are un program de protecție a acestora care este condus de Biroul Federal pentru Informații în Domeniul Securității.

Opinăm că o infrastructură critică reprezintă *un bun material care este vital pentru funcționarea economiei și a societății.*

Protecția unei infrastructuri critice este constituită din *totalitatea măsurilor stabilite pentru reducerea riscurilor de blocare a funcționării sau de distrugere a unei infrastructuri critice.*

Securitatea națională și internațională sunt dependente, în foarte mare măsură, de infrastructurile critice ale societății. Dar acesta sunt tot mai vulnerabile în fața mijloacelor din ce în ce mai sofisticate de atac asupra lor. Literatura de specialitate acordă spații ample pentru descrierea modalităților de protecție a infrastructurilor critice.

Sunt acceptate două axiome în analiza acestui domeniu:

- practic, este imposibil să se asigure protecția 100% a unei infrastructuri critice;
- nu există o soluție unică, universală pentru rezolvarea acestei probleme.

Specialiştii oferă trei moduri de abordare a protecţiei infrastructurilor critice:

1. Protecţia infrastructurilor critice informaţionale, care ia în consideraţie numai securitatea conexiunilor IT şi soluţiile de protecţie a acestora, competenţele protecţiei fizice a celorlalte infrastructuri fiind disipată între diverse organisme de stat sau private;

2. Asigurarea funcţionării neîntrerupte a reţelelor IT şi a elementelor fizice ale infrastructurilor critice. În acest caz, protecţia fizică reprezintă o componentă a sistemului naţional de protecţie civilă. În prezent, se încearcă o cooperare cât mai strânsă între sectorul public şi cel privat pentru atingerea unui grad cât mai înalt de protecţie a infrastructurilor critice. La nivel de planificare strategică, însă, cooperarea este aproape inexistentă. Acest tip de abordare a fost denumit generic "all hazards approach" (considerarea tuturor riscurilor);

3. Realizarea unui sistem minim obligatoriu de protecţie a sistemului de guvernare şi a anumitor organisme statale, vitale.

În ultimul timp, analiştii acordă atenţie sporită atacurilor cibernetice organizate, capabile să cauzeze destabilizarea infrastructurii naţionale, a economiei sau chiar a tuturor componentelor securităţii naţionale. Complexitatea tehnică solicitată pentru înfăptuirea unui astfel de atac este destul de ridicată şi, parţial, explică de ce încă nu s-au înregistrat astfel de atacuri până acum. Totuşi, nu trebuie să fim prea încrezători. Au fost cazuri în care atacanţii organizaţi au exploatat unele vulnerabilităţi care ne-au demonstrat că pot dispune şi chiar dispun de capabilităţi distructive şi mai mari. Să nu uităm că numai după o oră de cădere a sistemului de calculatoare al bursei din New York s-a creat, în iunie 2001, o panică generalizată şi o confuzie mondială.

Este cunoscut faptul că instrumentele şi metodologiile înfăptuirii atacurilor sunt larg răspândite, iar capacităţile

tehnice şi complexitatea utilizatorilor decişi să provoace un adevărat dezastru se află în creştere.

Pe timp de pace, persoane sau organizaţii interesate pot declanşa acte de sabotaj asupra instituţiilor statului, centrelor de cercetare ştiinţifică, companiilor private şi altor obiective strategice. Există posibilitatea pregătirii terenului pentru administrarea loviturilor din spaţiul cibernetic în cazul unei confruntări, prin cartografierea sistemelor informaţionale ale statului, identificând principalele ţinte şi plasând în infrastructura naţională porţi ascunse de intrare şi alte mijloace de acces.

Pe timp de criză sau război adversarii vor încerca să intimideze liderii politici naţionali prin atacarea infrastructurilor critice şi a funcţiilor de bază ale economiei sau prin erodarea încrederii publice în sistemele de conducere sau informaţionale.

Atacurile cibernetice asupra reţelelor informaţionale ale oricărei ţări pot avea consecinţe grave, cum ar fi întreruperea funcţionării unor componente-cheie, provocarea pierderilor de venituri şi proprietăţi intelectuale sau chiar pierderea vieţilor omeneşti. Contracararea unor astfel de atacuri este obligatorie şi necesită realizarea unor componente riguroase încă destul de anevoios de proiectat cu mijloacele existente azi.

1.2. Infrastructurile critice europene

Consiliul European, la reuniunea sa din iunie 2004[7], a cerut Comisiei Europene şi Înaltului Reprezentant să elaboreze o strategie globală privind consolidarea infrastructurilor critice şi protecţia cestora.

Problematica infrastructurilor critice se află de-acum şi în atenţia autorităţilor europene. De altfel, întregul spaţiu euro-atlantic şi-a redimensionat politica şi strategia cu privire la

[7] http://europa.eu.int/eurlex/lex/LexUriServ/site/fr/com/2004/com2004_0702fr01.pdf

securitatea şi securizarea infrastructurilor critice, îndeosebi după evenimentele dramatice de la 11 septembrie 2001 din Statele Unite ale Americii, dar şi din 11 martie 2004 de la Madrid şi din 2005 de la Londra. Aceste atacuri au confirmat ceea ce, de fapt, se ştia de multă vreme, şi anume faptul că societăţile moderne devin din ce în ce mai vulnerabile la atacuri teroriste şi la ameninţări asimetrice. Aceste atacuri afectează în special siguranţa persoanei fizice, adică a omului de pe stradă, şi securitatea infrastructurilor esenţiale, cele care reprezintă structura de rezistenţă a oricărei societăţi sau reţelele vitale ale funcţionării societăţii, ale vieţii de zi cu zi, ale siguranţei cetăţeanului şi instituţiilor.

Riscurile asociate posibilelor atentate teroriste la adresa infrastructurilor europene au crescut. Consecinţele unor astfel de atacuri se apreciază că ar fi variabile. Se estimează că un cyber-atac ar face puţine victime sau n-ar face deloc victime, dar ar putea duce la întreruperea funcţionării infrastructurilor vitale. Spre exemplu, un cyber-atac împotriva reţelei telefonice ar duce la întreruperea convorbirilor telefonice până la remedierea defecţiunii respective, iar acest lucru ar fi foarte grav, întrucât ar putea avea urmări în lanţ, imprevizibile. Există însă şi o altă perspectivă în ceea ce priveşte atacurile asupra infrastructurilor critice. Un atac asupra sistemelor de comandă-control ale instalaţiilor chimice sau ale reţelelor de gaze ar putea produce multe victime şi pagube materiale semnificative. Mai mult, efectele s-ar putea multiplica şi propaga în lanţ.

Un atac asupra reţelelor electrice ar putea avea efecte foarte mari, atât în funcţionarea întreprinderilor, reţelelor de calculatoare, reţelelor de comunicaţii etc., cât şi asupra aparaturii medicale vitale pentru supravieţuirea bolnavilor aflaţi în operaţii sau sub supraveghere monitorizată, acolo unde nu există surse proprii de energie electrică. Pana de curent survenită acum câţiva ani în America de Nord şi în Europa a

arătat că infrastructurile în domeniul energiei sunt deosebit de vulnerabile.

Infrastructurile critice sunt, potrivit unei definiţii europene, „*instalaţiile fizice şi tehnologice ale informaţiei, reţelele, serviciile şi activele care, în caz de oprire sau de distrugere, pot să producă incidente grave asupra sănătăţii, securităţii sau bunăstării economice a cetăţenilor sau activităţilor guvernelor statelor membre.*“[8]

Infrastructurile critice, potrivit documentului Comisiei Europene[9], înglobează:

- ❖ Instalaţii şi reţele din sectorul energiei (în special instalaţiile de producere a electricităţii, de petrol şi de gaze, instalaţiile de stocaj şi rafinăriile, sistemele de transport şi de distribuţie);
- ❖ Tehnologii de comunicaţii şi de informaţii (telecomunicaţiile, sistemele de radiodifuziune, programele, materialul informatic şi reţelele, inclusiv Internetul etc.);
- ❖ Finanţe (sectorul bancar, pieţele de valori şi investiţiile);
- ❖ Sectorul de îngrijire a sănătăţii (spitale, instalaţii de îngrijire a bolnavilor şi băncile de sânge, laboratoare şi produse farmaceutice, servicii de urgenţă, de căutare şi de salvare);
- ❖ Sectorul alimentar (securitate, mijloace de producţie, distribuţie şi industrie agroalimentară);
- ❖ Aprovizionarea cu apă (rezerve, stocaj, tratament şi reţele de distribuţie);
- ❖ Transporturi (aeroporturi, porturi, instalaţii intermodale, căi ferate, reţele de tranzit de masă, sisteme de control trafic);
- ❖ Producţie, stocaj şi transport ale produselor periculoase (materiale chimice, biologice, radiologice şi nucleare);

[8] Ibidem.
[9] Ibidem.

❖ Administrație (servicii de bază, instalații, rețele de informații, active, locuri importante, monumente naționale).

Aceste infrastructuri aparțin sectorului public sau celui privat. De aceea, în concepția Comisiei Europene, autoritatea publică trebuie să-şi asume responsabilitatea pentru consolidarea şi protecția acestor infrastructuri.

Infrastructurile critice trebuiau definite de fiecare stat membru al UE şi de UE, iar listele urmau să fie încheiate înainte de finele anului 2005.

În ceea ce priveşte infrastructurile critice, Uniunea Europeană are o situație specială, datorită unei istorii îndelungate şi foarte complexe şi, ca urmare, unor factori numeroşi, între care cei mai importanți sunt următorii:

- concentrarea întreprinderilor în mari localități;
- raționalismul industrial;
- fabricarea în flux continuu;
- interdependențele legate de producție, distribuție etc.;
- aglomerările urbane.

La acestea se adaugă rețelele moderne de comunicații, inclusiv rețeaua Internet, rețelele de calculatoare şi radionavigația prin satelit.

Aceste interdependențe fac să crească foarte mult vulnerabilitățile întregului sistem şi ale tuturor infrastructurilor critice. De aceea, este foarte posibil ca, în mod paradoxal, *paralel cu procesul de integrare europeană, numărul infrastructurilor critice să crească.* Aceasta este încă o concluzie foarte importantă pentru analiza infrastructurilor critice, a vulnerabilităților acestora şi, bineînțeles, a amenințărilor care se profilează în continuare la adresa lor.

Totuşi, infrastructurile critice nu sunt un dat. Ele cunosc o anumită dinamică, unele pot deveni critice, altele, securizate, pot ieşi din această categorie. Comisia Europeană sugerează trei criterii esențiale pentru identificarea potențialelor infrastructuri critice:

1. *Întinderea* sau *suprafața.* Deteriorarea infrastructurii critice este evaluată în funcție de regiunea geografică susceptibilă de a fi atinsă, de dimensiunea internațională, națională provincială/teritorială sau locală;
2. *Gradul de gravitate.* Incidența sau degradarea pot fi nule, minime, moderate sau ridicate. În continuare, se sugerează câteva criterii pentru evaluarea gradului de gravitate: incidența economică; incidența asupra publicului; incidența asupra mediului; dependența; incidența politică.
3. *Efectul în timp.* Acest criteriu indică momentul în care degradarea infrastructurii respective poate avea o incidență majoră sau un efect grav (imediat, după 24-48 de ore, într-o săptămână sau într-un termen mai lung).

Este datoria fiecărui stat să identifice, pe teritoriul său, infrastructurile critice. Dar statele europene nu sunt singure, izolate, ci în relații extrem de strânse, de complexe şi, de ce nu, de complicate. Dependențele şi interdependențele sunt atât de mari, încât nici un stat, în condițiile actuale şi în cele viitoare, nu va putea exista, şi supraviețui de unul singur. De altfel, acest concept de independență absolută a dispărut demult. Europa de azi este interdependentă. Lumea de azi devine din ce în ce mai mult interdependentă, deci responsabilă de tot ce întâmplă nu numai în relațiile internaționale, ci şi pe teritoriul fiecărui stat în parte. De aceea, procesul de identificare, de analiză, evaluare şi securizare (protecție) a infrastructurilor critice nu poate fi fragmentat şi, cu atât mai puțin, izolat. Dacă un singur stat nu-şi îndeplineşte obligațiile de a identifica, pe teritoriul său, infrastructurile critice şi de a lua, în context bilateral, regional, european, regional şi chiar global, măsurile ce se impun pentru reducerea vulnerabilităților acestora, pentru contracararea amenințărilor şi asigurarea standardelor de protecție şi de securitate necesare, efectele vor fi resimțite, într-o formă sau alta, de toate celelalte state, de întreaga regiune, de întregul continent sau chiar de întreaga lume.

Cu alte cuvinte, *responsabilitatea identificării, evaluării, protecției şi securizării infrastructurilor critice, în condițiile creşterii interdependențelor, accentuării vulnerabilităților şi proliferării amenințărilor la adresa acestora, capătă valențe şi*

valori internaționale, devenind o chestiune vitală pentru buna funcționare a societății. Aceasta este o altă concluzie importantă pentru gestionarea securității infrastructurilor critice.

Dimensiunea internațională a acestei responsabilități rezultă din următoarele realități:

- majoritatea infrastructurilor critice, sau care pot deveni critice, depăşeşte aria geografică a statelor politice;
- creşterea vulnerabilităților infrastructurilor critice dintr-un stat determină, într-o formă sau alta, creşterea vulnerabilității tuturor infrastructurilor critice din zonă sau din rețea;
- filosofia şi fizionomia de rețea accentuează inter-dependențele şi, în aceeaşi măsură, sporesc vulnerabilitățile tuturor structurilor participante, dar şi capacitatea şi forța de rezistență la perturbații şi amenințări.

Desigur, nu vor putea fi protejate complet şi în orice moment toate infrastructurile critice. Dar evaluarea amenințărilor la adresa acestora, a vulnerabilităților de sistem şi de proces la pericole şi amenințări, cooperarea internațională şi realizarea unui sistem european (regional, global) de identificare, monitorizare, evaluare, securizare şi protecție a infrastructurilor critice creează premise pentru ca securitatea infrastructurilor critice să poată fi gestionată în mod eficient.

Gestionarea securității este definită de Comisia Europeană ca un „*proces deliberat prin care se vizează evaluarea riscului şi punerea în operă a acțiunilor destinate să-l aducă la un nivel determinat şi acceptabil, cu un cost acceptabil*."[10]

Aceasta presupune:

- identificarea riscului asociat vulnerabilităților de sistem şi de proces al infrastructurilor critice, pericolelor şi amenințărilor la adresa acestora;
- analiza şi evaluarea de risc;
- controlul dinamicii acestuia;
- menținerea lui în limitele stabilite.

---

[10] Ibidem.

CAPITOLUL 2
DINAMICA INFRASTRUCTURILOR CRITICE

Infrastructurile sunt critice prin locul pe care îl au în cadrul unui sistem, prin rolul pe care îl joacă în cadrul stabilității şi funcționalității sistemului, prin gradul de expunere la uzură şi factori destabilizatori, dar şi prin mulțimea variabilă a vulnerabilităților lor (de sistem, de proces sau induse) la amenințările care le vizează nemijlocit sau care vizează, desigur tot în mod direct, sistemele sau procesele din care fac parte respectivele infrastructuri.

2.1. Factori ai dinamismului critic

De regulă, infrastructurile nu se construiesc pe bază de amenințări sau de vulnerabilități, deşi se ține totdeauna seama de un anumit standard de securitate intrinsecă a sistemului, ci în funcție de cerințele vitale – de stabilitate, deci, de stare, şi de funcționalitate, deci, de proces – ale sistemului, ale metasistemului (sistemului de sisteme) sau ale procesului din care fac parte. Spre exemplu, la realizarea rețelelor de distribuție a apei, se ține seama, în primul rând, de nevoile localității respective de aprovizionare cu apă, de condițiile concrete de realizare a distribuției (surse de apă potabilă, distanțe, trasee pentru conducte etc.), dar şi de securitatea acestor rețele, în sensul siguranței transportului apei, prevenirii avariilor, prevenire, limitare sau înlăturare a acțiunii factorilor nocivi etc. Probabil că, în viitor, va trebui să se țină seama şi de alți factori, cum ar fi, spre exemplu, protecția împotriva atacurilor de tip terorist, frecvența şi intensitatea unor calamități naturale, lunecări de teren şi de alți numeroşi agenți perturbatori. Infrastructurile critice sunt numeroase, diversificate şi dinamice. Practic, există atâtea infrastructuri critice câte sisteme şi procese, dar, de regulă, numai cele care

au un rol important în stabilitatea, securitatea şi siguranţa sistemelor şi proceselor sunt considerate astfel. Deşi mulţimea infrastructurilor critice este, în general, cunoscută *ab initio*, există şi o altă mulţime a infrastructurilor care devin critice pe parcurs şi o alta a infrastructurilor critice care îşi pierd această calitate în procesul evoluţiei sau involuţiei sistemului şi procesului din car fac parte.

Dinamismul infrastructurilor critice depinde de câţiva factori foarte importanţi printre care se situează şi următorii:

- variaţia (evoluţia, dezvoltarea, extinderea sau involuţia) sistemului sau procesului din care fac parte;
- gradul de integralitate a sistemului, de fluenţă, flexibilitate şi adaptabilitate a procesului;
- variaţia condiţiilor iniţiale ale mediului şi ale sistemului sau procesului;
- dinamica mediului şi a sistemelor de relaţie sau relaţionate sau corelaţionate;
- variaţia factorilor perturbatori.

Aceşti factori, dar şi alţii, influenţează transformările şi chiar mutaţiile care se produc în rândul infrastructurilor critice şi, de aceea, trebuie să se ţină seama de ei.

2.2. Tipologia infrastructurilor critice

Mulţimea infrastructurilor critice rămâne totdeauna deschisă şi variabilă. Aşa cum se sublinia mai sus, există atâtea infrastructuri critice câte sisteme şi procese, dar, pentru a sublinia mai bine această realitate, noi le vom împărţi în trei categorii mari, în funcţie de spaţiul-suport, mai exact de spaţialitatea lor, adică de spaţiul sau spaţiile în care sunt sau pot fi identificate. Ne vom referi, astfel la:

- infrastructurile din *spaţiul fizic*;
- infrastructurile din *spaţiul cosmic*;
- infrastructurile din *spaţiul virtual*.

Cu alte cuvinte, infrastructurile pot fi, într-o primă clasificare, *fizice*, *cosmice* şi *virtuale*.[11]

Aceste tipuri de infrastructuri, deşi se află în spaţii diferite, sunt strâns legate unele de altele, devenind din ce în ce mai mult interdependente, trans-sistemice, de metasistem sau de sistem de sisteme, şi complexe. Gradul lor de interdependenţă creşte foarte mult odată cu evoluţia vieţii pe pământ, iar al celor care ţin de sistemele politice, economice, financiare, sociale, informaţionale, culturale şi militare se consolidează în etapa globalizării, devenind o caracteristică esenţială a acestora. Această caracteristică, în mod logic, ar trebui să ducă la creşterea coeficientului de integralitate a tuturor infrastructurilor şi la restrângerea mulţimii infrastructurilor critice doar la cele care determină stabilitatea şi funcţionalitatea sistemelor. Din păcate, lucrurile, cel puţin pentru un timp previzibil, nu stau aşa. Interdependenţa şi integralitatea structurilor creează un nou tip de vulnerabilităţi pe care le vom numi, generic, *vulnerabilităţi de integralitate* sau *vulnerabilităţi de interdependenţe*. Spre exemplu, integrarea tuturor liniilor aeriene la nivel global, deşi duce automat la creşterea traficului aerian, a vitezei de transport, comprimând, deopotrivă, atât timpul, cât şi spaţiul, ar trebui să ducă, în mod automat, şi la reducerea vulnerabilităţilor de funcţionalitate şi de stabilitate şi la creşterea eficienţei transporturilor, ceea ce, de altfel, se şi întâmplă. În acelaşi timp, însă, liniile aeriene integrate la nivel planetar devin extrem de vulnerabile la atacuri teroriste, la calamităţi şi dezastre şi la alte pericole şi ameninţări asimetrice. Transporturile aeriene integrate la nivel mondial devin un sistem de

[11] Prof. dr. Jean Clarck, la conferinţa "Homeland Security Europe 2006", Bruxelles, 27-29 iunie 2006, face următoarea clasificarea infrastructurilor: *fizice* (reţele de apă, energie, transport, industrie chimică, sănătate publică, servicii de urgenţă, agricultură şi hrană); *informaţionale* (reţele, bănci şi finanţe, telecomunicaţii); *umane*; *bunuri-cheie* (nu sunt considerate critice, dar au valoare simbolică şi sunt importante pentru memoria colectivă: muzee, facilităţi guvernamentale şi comerciale).

sisteme, un metasistem, care intră în relaţie, pe de o parte, cu sistemele politice (care sunt statele), cu sistemele economice (globalizate, dar şi individualizate pe companii şi chiar pe state politice), cu sistemele informaţionale globalizate (dar extrem de vulnerabile) şi, pe de altă parte, cu reţelele şi entităţile ostile, perturbatoare, care sunt, de regulă, atipice sau asimetrice.

Considerăm că este foarte important să subliniem o astfel de realitate, întrucât, în acest fel, avem imaginea cât de cât realistă a unui labirint dinamic, cu evoluţii şi involuţii bruşte, care-şi schimbă deci structura în funcţie de factori perturbatori, de variaţia condiţiilor concrete şi a condiţiilor iniţiale şi de mulţi alţi factori, unii dintre ei foarte greu de identificat, de analizat, de cunoscut şi, evident, de influenţat.

De aici se desprinde o altă concluzie foarte importantă nu numai pentru acest studiu, ci şi pentru oricare alt efort de a identifica, optimiza şi securiza infrastructurile sistemelor dinamice complexe şi anume aceea că *vulnerabilităţile infrastructurilor critice cresc şi se transformă odată cu creşterea interdependenţei şi a gradului lor de integralitate*.

Infrastructuri critice din spaţiul fizic

Infrastructurile fizice sunt, totdeauna suporturi ale unor sisteme fizice complexe, de regulă, din spaţiul societăţii omeneşti, cu funcţii şi roluri sociale. Ele pot fi grupate, deci, pe categorii de sisteme fizice, astfel:

- **Infrastructuri critice ale întreprinderii**: reţea de distribuţie a energiei electrice de 380 volţi sau de înaltă tensiune; reţea de distribuţie a apei industriale; reţea de calculatoare; reţea de distribuţie a gazului metan, a carburantului sau altor substanţe şi materiale absolut necesare producţiei; reţeaua de comunicaţii (comandă-control); reţeaua depozitelor de materii prime şi de produse finite; reţeaua fizică de calculatoare (calculatoare, cabluri, conexiuni) etc.

- **Infrastructuri critice ale sectorului (ramurii)**: reţele de distribuţie a apei, energiei electrice, gazelor naturale folosite în procesul de producţie şi materialelor strategice între întreprinderi şi în cadrul ramurii; reţeaua depozitelor de materiale speciale (materiale strategice, materiale inflamabile; materiale radioactive, substanţe chimice, agenţi biologici şi alte materiale cu risc înalt); reţelele de comunicaţii, îndeosebi infrastructurile fizice ale acestora (relee, cabluri, suporţi, staţii etc.); reţelele de drumuri şi căi ferate: parcurile de maşini; reţelele fizice de calculatoare; bazele de date şi alte elemente vulnerabile sau cu rol important în funcţionarea întreprinderilor şi instituţiilor.
- **Infrastructuri critice ale economiei**: infrastructuri ale unor reţele de drumuri strategice; reţele şi, mai ales, noduri de căi ferate; reţele de producere şi distribuţie a energiei (infrastructurile sistemului energetic naţional); infrastructuri ale sistemelor de conducere; reţele de depozite de materiale strategice, de materii prime, de substanţe chimice, de material nuclear sau de agenţi biologici.
- **Infrastructuri critice ale transportului aerian**: aeroporturi; sisteme de aprovizionare cu energie, cu apă, cu gaze; reţele ale depozitelor de carburanţi; hangare şi parcuri de avioane; turnuri de control; infrastructuri control trafic aerian; reţele de calculatoare; staţii de radiolocaţie; staţii de dirijare la aterizare; alte infrastructuri ale sistemelor de care depind siguranţa şi securitatea zborului.
- **Infrastructuri critice ale transportului feroviar**: reţelele de căi ferate; poduri, viaducte şi ale lucrări de artă pe calea ferată sau adiacente acesteia; staţii; reţele electrice ale transportului feroviar; reţele de comunicaţii; alte tipuri de reţele.
- **Infrastructuri critice ale transportului naval**: porturi; infrastructuri portuare cu rol important, unic şi de neînlocuit în funcţionarea porturilor şi a transporturilor navale;

instalații de far; stații de radionavigație, stații de radiolocație; sisteme de comunicații; rețele de căi ferate și de drumuri importante din incinta porturilor; sisteme de diguri de protecție, alte infrastructuri ale sistemelor de securitate şi de siguranță a navigației pe mări şi pe fluvii;

➢ **Infrastructuri critice ale sistemului financiar**: sedii ale băncilor; suporți de informație; calculatoare; sisteme de protecție şi de siguranță; rețele de transport interbancar al banilor şi de bancomate; depozite.

➢ **Infrastructuri critice ale locuinței**; instalații electrice, de gaze şi de apă; sisteme de securitate a locuinței.

➢ **Infrastructuri critice ale localității**: rețele de transport al apei, energiei electrice şi gazelor, îndeosebi nodurile, punctele de control şi de distribuție; rețele ale transportului public (linii de metrou, linii de troleibuze, autobuze şi tramvaie, unele construcții şi diferite alte lucrări aferente importante); rețele telefonice, relee, stații şi centrale; relee şi posturi de radio şi de televiziune care se află în sistemul național sau local de alertă; iluminatul public; alimentarea cu energie termică; puțuri, stații şi alte infrastructuri ale sistemelor de purificare a apei; spitale de urgență şi alte infrastructuri ale medicinii şi asistenței medicale de urgență; laboratoare şi centre hematologice; infrastructuri ale sălilor de operații, sălilor de reanimare şi altor compartimente de supraveghere şi monitorizare a bolnavilor aflați în dificultate; infrastructuri ale sistemelor de prevenire şi stingere a incendiilor; infrastructuri ale sistemelor de protecție civilă, îndeosebi ale sistemelor şi rețelelor de acțiune şi de reacție în cazul unor calamități, dezastre, accidente nucleare, industriale, chimice şi tehnologice; rețele şi depozite etc.

➢ **Infrastructuri critice ale ținutului (județului, zonei etc.)**: rețele de căi ferate şi drumuri publice importante, îndeosebi centre vitale, adică noduri, stații, depozite, centre de comunicații etc.; rețele de depozite; conducte petroliere; rețele telefonice; relee ale sistemelor de comunicații prin microunde;

lucrări de artă, baraje, acumulări de ape, sisteme de canalizări şi de hidroameliorații cu impact vital asupra unor terenuri cultivate sau locuite; diguri şi alte infrastructuri pentru controlul inundațiilor şi revărsărilor; rețele de depozite de importanță locală, regională sau națională; elemente ale unor infrastructuri critice naționale sau internaționale; infrastructuri speciale.

➢ **Infrastructuri critice ale țării**: infrastructuri ale rețelelor sistemului național energetic (unități energetice, linii de înaltă tensiune, stații de transformare, instalații şi sisteme de monitorizare şi de reglare, baraje şi acumulări hidro-energetice; centrale nucleare, sisteme de infrastructuri ale acestor centrale nucleare, hidrocentrale şi termocentrale, combinate de apă grea, depozite de materii prime, materiale periculoase şi materiale strategice etc.); rețele de drumuri de importanță națională sau internațională; infrastructuri vitale ale acestor rețele; rețeaua feroviară cu toate structurile aferente (stații, depouri, rețele de aprovizionare a transportului feroviar cu energie electrică, material rulant, carburant şi alte materiale de importanță vitală, sisteme de comandă-control şi dirijare a traficului, infrastructuri ale sistemelor de comunicații feroviare etc.); rețeaua națională de transporturi aeriene, cu toate infrastructurile aferente; elemente de importanță vitală ale rețelelor internaționale de trafic aerian aflate pe teritoriul țării; infrastructuri ale transporturilor navale (porturi, infrastructuri portuare, diguri, infrastructuri pentru siguranța navigației, infrastructuri din zona litorală, instalații şi infrastructuri de far, radiofar şi ale altor sisteme de semnalizare); infrastructuri ale sistemului național de comunicații, dar şi ale altor sisteme de comunicații de importanță națională şi internațională (rețele telefonice, centrale de comunicații, noduri ale acestor rețele, echipamente de transport, trasee de fibră optică, relee, modulatori de semnal etc.); infrastructuri fizice ale rețelelor naționale de informații, de calculatoare, de televiziune etc.; infrastructuri ale rețelelor

naționale de alertă; rețele ale conductelor de petrol şi gaze naturale naționale sau care fac parte din rețele de transport continentale etc.

- **Infrastructuri critice ale continentului**: rețeaua europeană şi internațională de trafic aerian, cu toate infrastructurile aferente; rețeaua europeană de transport feroviar; infrastructuri ale rețelei europene de comunicații; infrastructuri ale traficului fluvial şi maritim (porturi, instalații portuare, sisteme de conducere şi de avertizare etc.); rețele de transport al petrolului şi gazelor naturale etc.
- **Infrastructuri critice internaționale**: infrastructuri ale traficului aerian internațional (radare, instalații aeroportuare, sisteme de control trafic, rețele de comunicații etc.); infrastructuri ale transporturilor maritime internaționale (sisteme de control şi dirijare a navigației, sisteme de semnalizare a zonelor periculoase, sisteme de comunicații, sateliți, instalații portuare cu funcții şi importante roluri internaționale, conducte de transport petrolier sau terminale ale acestora etc.); sisteme de comunicații internaționale; rețele de bănci etc.
- **Infrastructuri critice militare**: rețele de comunicații militare la nivel strategic şi la nivel tactic; infrastructuri ale acestor rețele; instalații de pe aerodromurile militare, din porturi militare, din baze militare şi din alte locații; rețele, conducte, depozite şi sisteme de aprovizionare cu carburanți, muniție, alimente şi ale produse de primă necesitate atât în timp de pact, cât şi la război sau în procesul participării la gestionarea crizelor şi conflictelor armate; infrastructuri rutiere, feroviare şi navale militare; rețele de depozite; arsenale; rețele de calculatoare; sisteme informatice.
- **Infrastructuri critice ale sistemului de ordine publică**: infrastructuri ale poliției şi jandarmeriei; infrastructuri ale pompierilor şi Inspectoratului pentru situații de urgență; infrastructuri ale forțelor şi formațiilor de reacție rapidă; infrastructuri critice ale sistemelor de protecție a cetățeanului, proprietății şi instituției.

- **Infrastructuri critice ale sistemului informațional şi de siguranță a statului**: infrastructuri ale serviciilor de informații şi ale altor instituții de care depinde protecția informațiilor, a intereselor naționale şi de alianță, a valorilor şi patrimoniului;
- **Infrastructuri critice ale sistemului sanitar şi de protecție a cetățeanului, familiei şi comunității**: rețele ale spitalelor de urgență; laboratoare; depozite de medicamente; infrastructuri ale unor centre de cercetări medicale etc.

Infrastructuri critice din spațiul cosmic

- **Infrastructuri critice ale spațiului cosmic**: stații orbitale; sateliți; sisteme de comunicații în spațiul cosmic etc.
- **Infrastructuri critice ale agențiilor şi altor structuri spațiale**: infrastructuri ale industriei spațiale; infrastructuri ale comunicațiilor din sistemul de pregătire şi efectuare a lansărilor şi traficului cosmic etc.

Infrastructuri critice din spațiul virtual

- Infrastructuri critice ale ciberspațiului;
- Infrastructuri critice ale sistemelor de comunicații;
- Infrastructuri critice ale rețelelor şi bazelor de date;

CAPITOLUL 3
AMENINȚĂRI LA ADRESA INFRASTRUCTURILOR CRITICE

Infrastructurile sunt sau devin critice datorită, în primul rând vulnerabilității lor la acele amenințări care le vizează în mod direct sau sunt îndreptate împotriva sistemelor, acțiunilor şi proceselor din care fac parte.

Amenințările la adresa infrastructurilor critice sunt condiționate, favorizate şi facilitate de cel puțin trei factori foarte importanți:

- lipsa de flexibilitate, dată de caracterul fix şi de locația relativ exactă a infrastructurilor, inclusiv a celor critice;
- flexibilitatea, fluiditatea, perversitatea pericolelor şi amenințărilor la adresa infrastructurilor critice şi spectrul foarte larg de manifestare a acestora;
- caracterul greu previzibil şi surprinzător ale pericolelor şi amenințărilor la adresa infrastructurilor critice.

De asemenea, pericolele şi amenințările la adresa infrastructurilor critice pot fi grupate în funcție de locația acestor infrastructuri, de forma de manifestare, de sfera de cuprindere, de modul în care ele apar şi se dezvoltă etc.

3.1. Tipologia pericolelor şi amenințărilor la adresa infrastructurilor critice

Unele dintre aceste pericole şi amenințări fac parte din natura lucrurilor, sunt pericole şi amenințări de sistem sau de proces, fiind un efect al disfuncțiunilor sau un produs al evoluției sistemelor şi proceselor. Altele sunt provocate în mod intenționat, ca urmare a anumitor interese, a bătăliei permanente şi necruțătoare pentru putere şi influență, adică pentru resurse, piețe şi bani.

Considerăm că pericolele şi amenințările la adresa infrastructurilor critice ar putea fi grupate astfel:

- pericole şi amenințări cosmice, climatice şi geofizice;
- pericole şi amenințări rezultate din activitatea oamenilor;
- pericole şi amenințări asupra infrastructurilor critice din spațiul virtual.

3.1.1. Pericole şi amenințări cosmice, climatice şi geofizice

Aceste pericole[12] şi amenințări[13] rezultă, de regulă, din dinamica fizică a pământului, din cea haotică a fenomenelor meteorologice şi chiar cosmice, dar şi din capacitatea posibilă a omului de a produce astfel de pericole şi amenințări şi a le folosi ca arme cosmice, climatice sau geofizice.

Printre principalele *pericole şi amenințări cosmice* la adresa infastructurilor critice fizice ar putea fi situate şi următoarele:

a) Naturale:

- căderi de meteoriți;
- intensificarea radiației solare şi a celei cosmice, în condițiile în care puterea de reacție şi de absorbție a ionosferei scade semnificativ;

---

[12] Înțelegem prin *pericol* o disfuncțiune gravă şi primejdioasă a unui sistem şi proces (pentru acel sistem sau proces, dar şi pentru altele aflate în relație cu acestea sau în împrejurimi).

[13] Amenințarea este un pericol direct, orientat, adică un pericol care vizează un anume sistem, un anume proces, o persoană, o instituție, o țară, o alianță, un proces etc. Apar, în cadrul amenințării, cui anume se adresează un anume pericol, adică direcționalitatea şi chiar intenționalitatea. Spre exemplu, uraganul declanşat într-un anume punct al Pacificului afectează coastele Californiei şi nu pe cele ale Americii Latine. Pentru coastele Californiei, uraganul respectiv este o amenințare. Acest uragan este însă produs de natură, în timp ce declanşarea unei încărcături explozive într-un mediu aglomerat, care amenință deci viața tuturor celor care întâmplător se află acolo, este efectuată de un terorist sau de către o grupare teroristă cu un anume scop.

- intensificarea ciclului solar;
- furtunile cosmice şi alte fenomene care afectează sau pot afecta în mod direct şi planeta noastră.

b) Produse:

- acţiuni din spaţiul cosmic îndreptate împotriva unor infrastructuri critice, în situaţia în care pătrund în Cosmos arme şi alte mijloace ce pot fi folosite pentru realizarea unor obiective sau materializarea unor interese;
- acţiuni asupra unor infrastructuri critice aflate chiar în acest spaţiu;
- un posibil terorism cosmic.

Pericolele şi ameninţările climatice sunt mult mai frecvente şi mai numeroase decât cele cosmice. Ele fac parte din viaţa noastră şi afectează, practic, aproape toate structurile fizice critice, creând probleme numeroase, frecvente şi foarte grave pentru infrastructurilor critice[14] din întreaga lume.

Sfera acestor pericole şi ameninţări este foarte largă, cu evoluţii bruşte, haotice şi imprevizibile. Printre principalele pericole şi ameninţări climatice şi meteorologice ar putea fi situate şi următoarele:

a) Naturale:

- încălzirea planetei;
- topirea gheţarilor şi creşterea nivelului oceanelor;
- uragane, furtuni şi alte fenomene meteorologice;
- precipitaţii masive, îndeosebi ploaie şi grindină;
- căderi masive de zăpadă, avalanşe, distrugerea echilibrului termic al unor zone întinse şi a infrastructurilor aflate aici;
- ploi acide;
- inundaţii şi mari revărsări de ape;
- modificarea albiilor unor fluvii şi râuri;
- apariţia unor fluvii şi râuri subterane;

[14] Una dintre cauzele pentru care infrastructurile devin critice este tocmai vulnerabilitatea lor la astfel de fenomene.

- împuţinarea rezervelor de apă potabilă;
- deşertizarea[15];
- sărăturizarea solurilor etc.

b) Produse:

- schimbarea regimului pluvionar, datorită tăierii masive a pădurilor şi distrugerii echilibrului ecologice, a ecosistemelor şi a ciclurilor trofice;
- exploatarea iraţională a unor soluri şi crearea unor dezechilibre grave;
- producerea de ploi artificiale;
- intervenţia în fenomenele meteorologice[16] şi chiar climatice etc.;
- incendierea pădurilor;
- terorismul meteorologic.

Fără îndoială, *pericolele şi ameninţările geofizice* rezultă din dinamica planetei, din faptul că pământul „lucrează" în fiecare minut, în toate dimensiunile sale, de la aşezarea pe nucleu, până la mişcările plăcilor tectonice şi recompunerea mai mult sau mai puţin înceată a substanţelor şi elementelor din care este format.

Cele mai frecvente pericole şi ameninţări de acest fel ar putea fi:

a) Naturale:

- cutremure;
- erupţii vulcanice;
- modificarea fundului oceanelor;

[15] Această ameninţare foarte gravă este prezentă şi în România, datorită tăierii masive a pădurilor şi distrugerii sistemelor de irigaţii.

[16] În unele publicaţii, se apreciază că programul HAARP, ca şi alte programe asemănătoare care studiază comportamentul ionosferei la bombardarea cu radiaţii de înaltă frecvenţă, ar putea fi la originea unor fenomene meteorologice dirijate de foarte mare amploare (precipitaţii masive, crearea unor nuclee de ciclon etc.), care ar putea avea valoarea unei adevărate arme meteorologice, care ar face parte dintr-un sistem de arme neconvenţionale, cosmice, climatice şi geofizice, bazate pe amplificarea de aproape două milioane de ori a undelor.

- fenomene de tipul tsunami;
- surpări de teren, rupturi şi falii imense etc.

b) Produse:

- lunecări de teren[17];
- scufundări de teren;
- cutremure[18];
- terorism geofizic.

3.1.2. Pericole şi ameninţări rezultate din activitatea oamenilor

Din păcate, cele mai multe dintre pericolele şi ameninţările care afectează în mod grav infrastructurile critice se datorează oamenilor.

Aceste tipuri de pericole şi ameninţări pot fi încadrate în două mari categorii:

- intrinseci activităţii omeneşti;
- ca mijloace neconvenţionale de confruntare (de luptă).

Cele *intrinseci activităţii omeneşti* pot fi:

a) de sistem;
b) de proces;
c) de dinamică.

a) Principale *pericole şi ameninţări la adresa infrastructurilor critice rezultate din disfuncţionalităţile de sistem* sunt generate chiar de sistemele de infrastructuri sau de sistemele din care acestea fac parte, în calitatea lor de metasisteme sau de sisteme de sisteme.

[17] Datorită defrişărilor necontrolate de păduri, exploatării iraţionale a subsolului, lipsei unor minime lucrări de protecţie, experimentelor nucleare etc.

[18] Este puţin probabil că omul a ajuns la o asemenea performanţă încât să producă fenomene geofizice grave, precum cutremure de pământ sau mişcarea voluntară a plăcilor tectonice. Nu trebuie însă exclusă nici o asemenea de posibilitate. S-a demonstrat că, spre exemplu, o explozie nucleară subterană produsă într-o anumită zonă (vulcanică, de falii la suprafaţă etc.) ar putea genera cutremure şi alte fenomene geofizice de o anumită intensitate.

Aceste tipuri de ameninţări sunt foarte numeroase şi greu de evitat, întrucât unele sunt fireşti, iar altele imprevizibile. Practic, există atâtea pericole şi ameninţări câte sisteme. Printre cele mai importante s-ar putea situa şi următoarele:

- îmbătrânirea şi degradarea infrastructurilor, mai exact, tendinţa unora dintre infrastructuri de a se uza prematur fizic şi moral, datorită vulnerabilităţilor sporite, expunerii îndelungate şi lipsei de protecţie sau protecţiei insuficiente;
- evoluţia sistemului spre o nouă stare şi, ca atare, ameninţarea cu distrugerea unora dintre propriile sale infrastructuri (introducerea fibrei optice duce, automat, la degradarea prea grăbită a liniilor telefonice tradiţionale şi a altor purtători de semnal);
- apariţia bruscă a unor disfuncţionalităţi în sistem (distrugerea intempestivă sau accidentală a unor componente sau a unor structuri etc.);
- efectul de bumerang;
- rezultate din evoluţia altor sisteme, din presiunea exercitată de acestea sau ca urmare a disfuncţionalităţilor din cadrul acestora, intenţionat sau neintenţionat etc.

b) *Pericolele şi ameninţările specifice proceselor fizice şi sociale* sunt cele mai complexe şi cu efectele cele mai mari. Ele se manifestă, de regulă, surprinzător şi intempestiv şi pot avea efecte distrugătoare foarte greu de contracarat. Printre cele mai importante pericole şi ameninţări de proces s-ar putea situa şi următoarele:

- schimbările în desfăşurarea unor activităţi ca urmare a acţiunii a numeroşi factori perturbatori;
- acţiuni economice, financiare şi de altă natură pentru distrugerea concurenţei;
- bătălii pentru resurse şi pentru pieţe;
- ofensiva *high-tech* şi *IT*;
- rezistenţa la ofensiva tehnologică şi informaţională şi riposta asimetrică;
- înarmarea;
- dezvoltarea unor sisteme de arme neconvenţionale care pot fi folosite împotriva infrastructurilor critice;

- acţiuni ale lumii interlope, traficanţilor şi reţelelor crimei organizate;
- terorism.

c) *Pericolele şi ameninţările de dinamică* îmbracă toate formele enunţate mai sus, dar şi foarte multe altele care rezultă, în general, din filosofia şi fizionomia sistemelor şi proceselor dinamice complexe. Printre cele mai frecvente considerăm că ar putea fi:

- variaţiile bruşte în funcţionarea şi comportamentul sistemelor şi în desfăşurarea proceselor;
- variaţia rapidă a intercondiţionărilor dintre sisteme, fenomene şi procese, datorată schimbărilor condiţiilor interne şi de mediu;
- variaţia intempestivă a condiţiilor iniţiale;
- acţiunea unor factori perturbatori imprevizibili;
- terorism dinamic complex.

3.1.3. Pericole şi ameninţări asupra infrastructurilor critice din spaţiul virtual.

Pericolele şi ameninţările din spaţiul virtual vizează, în general, reţelele, nodurile de reţea şi centrele vitale, mai exact, echipamentele şi sistemele fizice ale acestora (calculatoare, providere, conexiuni şi noduri de reţea etc.), precum şi celelalte infrastructuri care adăpostesc astfel de mijloace (clădiri, reţele de energie electrică, cabluri, fibră optică şi alte componente). În aceeaşi măsură, ele vizează şi depozitele de date şi de programe, sistemele de înmagazinare, de păstrare şi de distribuţie a informaţiei, suportul material al bazele de date şi multe altele. Însă, înainte de toate, asemenea pericole şi ameninţări vizează sistemele IT (întreprinderi, linii de producţie, sisteme de aprovizionare cu materiale strategice, infrastructuri de resurse şi de pieţe, institute de cercetări, sisteme de comunicaţii).

Din categoria, mereu în extensie, a pericolelor şi ameninţărilor împotriva infrastructurile critice ale ciberspaţiului fac parte şi următoarele:

- pericolele şi ameninţările rezultate din bătălia dintre marile firme pentru supremaţia IT, pentru resurse şi pentru pieţe;
- pericolele şi ameninţările asimetrice;
- dezvoltarea reţelelor subversive şi neconvenţionale IT;
- activitatea tot mai intensă a hacker-ilor;
- ciberterorismul.

3.2. Dinamica pericolelor şi ameninţărilor la adresa infrastructurilor critice

Toate pericolele şi ameninţările enunţate mai sus, dar şi altele, care se pot ivi pe neaşteptate, vizează în mod direct, în primul rând, oamenii şi infrastructurile. Cele care suportă direct şi aproape fără posibilitate de reacţie eficientă aceste ameninţări sunt denumite infrastructuri critice. Între mulţimea deschisă a infrastructurilor critice şi mulţimea pericolelor şi ameninţărilor la adresa acestora se creează totdeauna relaţii de intercondiţionare directă, intempestivă, bine cunoscută sau aleatoare, ceea ce face extrem de dificile politicile, strategiile şi practicile de protecţie.

Filosofia şi fizionomia infrastructurilor critice – în general, infrastructuri de reţea – sunt definite pe un determinism dinamic complex, ceea ce impune o monitorizare atentă, o analiză permanentă şi o evaluare pe măsură a raporturilor şi interinfluenţelor.

Odată cu dezvoltarea pericolelor şi ameninţărilor asimetrice[19], cu intensificarea acţiunilor teroriste, problematica arhi-

[19] *Pericolele şi ameninţările simetrice* rezultă din confruntarea sau posibilitatea de confruntare a două entităţi aproximativ egale, simetrice sau asemănătoare. *Pericolele şi ameninţările disimetrice sau non-simetrice* provin din efectul de disproporţionalitate, creat de marile decalaje din toate domeniile inclusiv din cele care privesc infrastructurile critice. *Pericolele şi ameninţările asimetrice* rezultă din efectul de adaptare la disproporţionalitate şi, respectiv, din crearea posibilităţii şi probabilităţii condiţionate ca fiecare dintre părţi dă poate distruge, prin mijloace specifice, infrastructurile critice ale celeilalte.

tecturii, alcătuirii, construcției, funcționării şi protecției infrastructurilor critice devine extrem de complexă şi necesită o abordare pe măsură, cu implicarea statelor, alianțelor, organizațiilor şi organismelor internaționale. Globalizarea informației, economiei şi relațiilor dintre state, dezvoltarea rețelelor de informații şi comunicații, concomitent cu recrudescența fenomenelor cosmice, climatice, meteorologice şi geofizice, impun abordări de amploare, ceea ce determină politici şi strategii pe măsură în tot acest spectru, de la identificare şi cunoaştere, la monitorizare, evaluare, prognozare şi protecție.

CAPITOLUL 4
PROTECȚIA, SIGURANȚA ŞI SECURITATEA INFRASTRUCTURILOR CRITICE

Protecția, siguranța şi securitatea infrastructurilor critice presupun cel puțin trei abordări complementare:

- ca funcție intrinsecă sistemelor, acțiunilor şi proceselor;
- ca sistem de securitate adiacent, asociat, creat de alte structuri;
- ca funcție de metasistem sau de sistem de sisteme.

Protecția infrastructurilor critice (PIC) presupune un parteneriat continuu şi coerent între proprietarii infrastructurilor critice, personalul care le deserveşte sau le gestionează şi autoritățile statului respectiv şi cele ale statelor membre ale Uniunii Europene (regionale) sau ale tuturor statelor (în situația în care este vorba de infrastructuri critice de valoare şi importanță mondială, cum ar fi, spre exemplu, protecția infrastructurilor care asigură transporturile aeriene, cele ale rețelelor de comunicații şi informații etc.).

Evident, primii responsabili pentru protecția respectivelor infrastructuri (instalații fizice, căi de aprovizionare,

tehnologii de informații, rețele de comunicații) sunt proprietarii şi personalul care le deservesc.

Există o bogată legislație națională, europeană şi internațională care se referă la funcționarea şi protecția infrastructurilor critice, precum şi la controlul necesar. Spre exemplu, inspecțiile desfăşurate în cadrul tratatului EURATM au vizat asigurarea utilizării în bune condiții şi în siguranță a materialelor nucleare.

A fost, de asemenea, creată o Agenție europeană însărcinată cu securitatea rețelelor şi informației (ENISA). Obiectivul principal al acestei Agenții este asigurarea securității comunicațiilor.

4.1. Programul european de protecție a infrastructurilor critice (EPCIP)

În realizarea şi implementarea unui program european de protecție a infrastructurilor critice s-a pornit de la o realitate complexă şi de la o concluzie pe măsură: *este imposibil ca Uniunea Europeană să poată realiza, de facto, protecția tuturor infrastructurilor critice.* De aceea, programul are în vedere numai infrastructurile critice transnaționale, protecția celor naționale rămânând în responsabilitatea statelor membre ale UE, dar, evident, într-un cadru comun. În acest sens, există deja numeroase directive şi reglementări, care impun mijloace şi proceduri pentru sesizarea accidentelor, elaborarea unor planuri de intervenție, în colaborare cu protecția civilă, cu administrația, cu serviciile de urgență etc. Există, spre exemplu, o mulțime de programe de acțiune şi de reacție în urgențe civile şi militare, cum ar fi accidentele nucleare, industriale, chimice, petroliere, ecologice, catastrofele naturale etc.

Comisia Europeană ține o evidență strictă a acestora, informează şi raportează în fiecare an situația în ceea ce priveşte evaluarea riscurilor, dezvoltarea tehnicilor de protecție

şi acţiunile juridice. Comisia propune actualizarea măsurilor, adică armonizarea, coordonarea şi colaborarea pe orizontală.

Această comunicare a Comisiei Europene, în care se înglobează toate analizele şi măsurile sectoriale, constituie baza unui *program european de protecţie a infrastructurilor critice* (EPCIP). Programul trebuie să identifice infrastructurile critice, să le analizeze vulnerabilităţile, dependenţele şi interdependenţele şi să găsească soluţii pentru securizarea acestora.

Obiectivele programului sunt următoarele:

- Identificarea şi inventarierea, prin guvernele statelor membre, a infrastructurilor critice situate pe teritoriile fiecărui stat, în funcţie de priorităţile stabilite prin EPCIP;
- Colaborarea întreprinderilor, în cadrul sectoarelor respective şi cu guvernele pentru diseminarea informaţiei şi reducerea riscului unor incidente susceptibile de a produce perturbaţii extinse sau durabile infrastructurilor critice;
- Abordarea comună a problemei securităţii infrastructurilor critice, graţie colaborării tuturor actorilor publici şi privaţi.

Programul european are în vedere, între altele, reunirea, într-o reţea, a tuturor specialiştilor în protecţia infrastructurilor critice din statele membre ale UE. Aceasta ar putea contribui la realizarea unei reţele de alertă în ceea ce priveşte structurile critice (Critical Infrastructure Warning Information Network – CIWIN). Reţeaua a fost pusă deja în funcţiune în 2005. Funcţia principală a acestei reţele este aceea de a contribui la încurajarea schimbului de informaţii privind ameninţările şi vulnerabilităţile comune, la realizarea unui schimb de măsuri şi de strategii adecvate, care să permită limitarea riscurilor şi protejarea infrastructurilor critice.

Programul EPCIP ajută statele, proprietarii şi utilizatorii infrastructurilor critice. În acest sens, Comitetul European de Normalizare (CEN) şi alte organisme de normalizare sprijină

reţeaua (CIWIN), propunând norme de securitate sectorială uniforme şi adaptate pentru toate sectoarele vizate.

4.2. Cooperarea internaţională în protecţia infrastructurilor critice

Perspectiva din ce în ce mai ameninţătoare a acţiunilor teroriste, înmulţirea şi diversificarea dezastrelor naturale şi posibilităţile de producere a unor accidente tehnologice cu consecinţe majore au impus în ultimii ani concentrarea atenţiei asupra protecţiei infrastructurilor critice (PIC). Aceasta este cu atât mai profundă cu cât interdependenţele de natură naţională, dar mai ales internaţională a infrastructurilor industriale, cibernetice, de comunicaţii, transport, energetice, bancare etc. au devenit greu de substituit. În ciuda faptului că modalităţile de abordare a protecţiei structurilor critice diferă de la o ţară la alta, de la o organizaţie la alta, se pot identifica elemente structurale comune, măsuri concertate desfăşurate cu succes, funcţii şi responsabilităţi compatibile.

Organizaţia de Cooperare şi Dezvoltare Economică (OCDE) tratează problema PIC din punctul de vedere al incidentelor economice şi catastrofelor. Măsurile se referă în special la restabilirea comunicaţiilor în cazul cutremurelor de pământ, asigurarea fluenţei traficului în caz de catastrofe naturale, securitatea în domeniul maritim, înlăturarea efectelor accidentelor chimice etc.

În cadrul Uniunii Europene, *Consiliul Europei* a realizat „acordul parţial deschis privind riscurile majore” care are ca scop cooperarea în domeniul gestionării riscurilor. Se preocupă, de asemenea, de formarea unui culturi a riscului prin organizarea de cursuri universitare şi masterate. În octombrie 2004, Comisia Europeană a adoptat un document referitor la protecţia

infrastructurilor critice[20], care propune măsuri suplimentare de întărire a instrumentelor existente, în special, punerea în aplicare a unui program european de protecţie (EPCIP). În cadrul acestuia a fost constituit un forum permanent pentru realizarea unui echilibru, pe de o parte, între constrângerile impuse de concurenţă, responsabilitate în gestionarea informaţiilor şi, pe de altă parte, de avantajele ce decurg din realizarea unui sistem de protecţie eficient pentru infrastructurile critice.

Din această perspectivă, Comisia Europeană şi-a propus să realizeze şi un sistem de avertizare pentru infrastructurile critice (CIWIN – Critical Infrastructure Warning Information Network).

La începutul anului 2005, Comisia Europeană şi *Agenţia Spaţială Europeană* (ESA) au organizat un forum internaţional de mare amploare, unde au fost invitate cele mai importante agenţii spaţiale. Tema reuniunii a fost întărirea cooperării în vederea prevenirii unor dezastre naturale sau accidente tehnologice majore şi a facilitării operaţiilor de salvare printr-o supraveghere cât mai extinsă a planetei prin intermediul sateliţilor. De altfel, încă din 2001, Comisia Europeană a lansat iniţiativa GMES - supraveghere globală pentru mediu şi securitate – care are ca obiectiv realizarea, până în 2008, a unor capabilităţi operaţionale autonome de monitorizare a mediului.

Organizaţia Internaţională pentru Protecţia Civilă (OIPC) este o federaţie de structuri naţionale de protecţie civilă. Aceasta se doreşte o platformă de comunicare, de schimburi de experienţe şi de cooperare în domeniu. Una din atribuţiile sale majore o reprezintă standardizarea procedurilor de urgenţă.

Comisia Economică pentru Europa din cadrul ONU a stabilit o serie de norme şi standarde în domeniul infrastructurilor, al transporturilor de materiale periculoase şi al accidentelor transfrontaliere.

[20] www.isn.ethz.ch/cr.n.

G8 dezvoltă politici de protecţie a infrastructurilor critice. La summit-ul din 2003 a adoptat un text care cuprinde 11 principii directoare ce asigură statelor membre, dar şi altor ţări, un cadru de dezvoltare a strategiilor de protecţie a infrastructurilor critice, în special în domeniul informatic.

Organizaţia pentru Securitate şi Cooperare în Europa (OSCE), ca şi celelalte organizaţii internaţionale, se află în plin proces de definire a unor noi atribuţii şi structuri care să corespundă fenomenului de globalizare şi noilor tipuri de riscuri şi ameninţări. La Conferinţa Anuală de Revizuire a Securităţii din 2004 s-a pus problema intensificării schimbului de informaţii privind riscurile şi reacţia coordonată în domeniul PIC. Astfel, o prima măsură stabilită este organizarea de reuniuni ale experţilor, având ca finalitate imediată redactarea unui set de recomandări ale OSCE, pe baza cărora să se poată realiza o adevărată „securitate teritorială OSCE”.

Centrul pentru Politici de Securitate de la Geneva a organizat, la sfârşitul anului 2003, un forum dedicat coordonării în domeniul PIC. A fost primul forum de acest gen, la care au participat peste 180 de experţi din 28 de ţări. Concluziile au fost extrem de interesante, ele referindu-se la tendinţele generale ale PIC, soluţiile greşite la care s-a apelat până în prezent şi modalităţile de „a gândi diferit”, de „a gândi imposibilul” şi de „a schimba mentalităţile”.

La 5 noiembrie 2005 a fost adoptat Programul de la Haye[21], în care se prevedea, între altele, consolidarea măsurilor pentru gestionarea crizelor transfrontaliere, protecţia infrastructurilor vitale şi a problemelor ce ţin de tensiunile şi conflictualitatea specifică ordinii publice şi securităţii. În acest sens, Consiliul European a încredinţat Comisiei Europene şi, respectiv, structurilor din cadrul Consiliului, sarcina realizării unui dispozitiv integrat al UE, care să devină operaţional cel mai târziu în iulie 2006. Dispozitivul, potrivit programului adoptat, trebuie să evalueze capacităţile statelor membre

[21] Adus la zi pe 17 decembrie 2004 pe probleme specifice luptei împotriva terorismului.

ale UE, să asigure pregătirea şi desfăşurarea unor exerciţii comune şi să întocmească un plan operaţional comun pentru o gestionare civilă a crizelor. El trebuie să realizeze, între altele:

- protecţia cetăţenilor şi infrastructurilor împotriva pericolelor şi ameninţărilor teroriste CRBN, în spaţiile publice, dar şi împotriva catastrofelor naturale (seisme, inundaţii, incendii de păduri) şi catastrofelor tehnologice, maritime, de transport, sanitare etc., în cadrul unei strategii europene integrate, printr-un dispozitiv de reacţie bine structurat şi interoperaţional;
- promovarea unor norme de securitate comune, la nivel UE, stabilirea unor scenarii şi exerciţii de pregătire şi de punere în aplicare a unor mecanisme de gestionare a crizelor, de alertă rapidă şi de protecţie civilă;
- realizarea unui sistem de reacţie rapidă şi eficientă împotriva atacurilor teroriste asupra infrastructurilor şi pentru lichidarea urmărilor acestora, care să garanteze revenirea în scurt timp la normalitate;
- întrucât infrastructurile europene sunt din ce în ce mai mult interconectate şi interdependente, este nevoie de o politică şi o strategie unitare, care să folosească toate pârghiile statelor şi UE pentru protecţia acestora.

Consiliul a făcut următoarele recomandări:

a) punerea deplină în operă a recomandărilor Consiliului European privind stabilirea unui „mecanism integrat de gestionare a crizelor în UE“, esenţial pentru întărirea legăturilor între cetăţenii şi instituţiile europene şi strângerea legăturilor de interdependenţă şi de solidaritate între statele membre;

b) centrarea strategiei europene integrate pe contracararea ameninţărilor asupra infrastructurilor vitale a căror distrugere ar putea avea efecte grave asupra sănătăţii, securităţii, siguranţei şi bunăstării economice a cetăţenilor, punerea în aplicare şi armonizarea la nivel european a unei metode armonioase prin care să se identifice infrastructurilor vitale, să se analizeze vulnerabilităţile, să se evalueze ameninţările şi să se propună soluţii viabile pentru protecţia acestora;

c) instituirea unui Program european de protecţie a infrastructurilor vitale (EPCIP);

d) considerarea programului european ca fiind complementar programelor naţionale;

e) admiterea situaţiei potrivit căreia:

- un sistem european de analiză a riscurilor trebuie să fie conceput şi pus în aplicare;
- realizarea unor legături strânse între toate autorităţile care deţin informaţii şi care au competenţe în acest domeniu;
- gestionarea corectă şi fiabilă a informaţiilor pertinente (informaţii militare şi civile, cooperare poliţienească), control parlamentar;
- crearea, în sânul Comisiei, a unui sistem de alertă rapidă în caz de criză, la nivel european, naţional şi internaţional partajat printr-o reţea centrală (ARGUS);
- asocierea Comitetului European de Normalizare;

f) a veghea ca Programul European de Protecţie a Infrastructurilor Critice (EPCIP) să respecte următoarele condiţii:

- să fie plasat sub controlul parlamentului european şi parlamentelor naţionale;
- să constituie un element esenţial al viitorului dispozitiv continental şi mondial de protecţie a infrastructurilor critice;

g) ameliorarea Fondului European de Solidaritate (pentru intervenţii în interiorul UE) şi ECHO (pentru intervenţii în afara UE);

h) crearea unei Forţe Europene de Protecţie Civilă;

i) consolidarea parteneriatului cu societatea civilă pentru realizarea unei strategii privind protecţia împotriva ameninţărilor CBRN;

j) asigurarea condiţiilor pentru ca toate aceste sisteme de alertă în caz de urgenţe civile şi militare şi de protecţie să nu afecteze viaţa cetăţenilor şi siguranţa lor, să nu îngrijoreze şi să panicheze în mod inutil populaţia;

k) garantarea respectului vieţii private, protecţia informaţiei şi prevenirea difuzării ei neautorizate;

l) elaborarea unui dispozitiv-cadru european de protecţie şi nedivulgare a datelor, astfel încât drepturile fundamentale ale omului să fie protejate;

m) asigurarea condiţiilor ca protecţia populaţiei şi a infrastructurilor vitale să se bazeze pe scenarii realiste şi pe

experienţe verificate (spre exemplu, experienţa dobândită în timpul Jocurilor Olimpice de la Atena din 2004).

Aceste reglementări şi experienţe se regăsesc, într-o formă sau alta, în strategiile naţionale de protecţie a populaţiei şi infrastructurile vitale ale tuturor ţărilor europene. În Germania, spre exemplu, există aşa-numitul concept *de protecţie de bază*[22]. Punctul de plecare îl reprezintă un proces de analiză şi de planificare multietajată, care cuprinde o evaluare a pericolelor, ameninţărilor şi riscurilor asociate, urmată de un control şi de o adaptare a măsurilor de protecţie.

Acest concept german presupune[23]:

I. identificarea diferitelor categorii de riscuri din diferite domenii: catastrofe naturale, accidente, terorism şi criminalitate;
II. fixarea nivelului de protecţie bazat pe aceste categorii;
III. conceperea de scenarii ale sinistrelor şi ameninţărilor;
IV. analiza punctelor slabe;
V. formularea obiectivelor de protecţie şi fixarea măsurilor de protecţie şi contra-protecţie care decurg de aici;
VI. formularea urgenţelor (coordonarea între măsurile publice şi private);
VII. punerea în aplicare, după nevoi, a acţiunii formulate;
VIII. controlul sistematic al acestui proces de analiză şi planificare în cadrul gestionării calităţii.

4.3. Protecţia infrastructurilor critice naţionale

Protecţia infrastructurilor vitale (critice) naţionale româneşti se înscrie, într-o formă sau alta, în programul

[22] Protecţia Infrastructurilor Critice – Concept de bază.

[23] Oficiul Federal pentru Protecţia Populaţiei şi Gestionarea Catastrofelor *(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)*, Centrul de Protecţie a Infrastructurilor Critice *(Zentrum Schutz Kritischer Infrastrukturen)*, Deutschherrenstrasse 93-95 53177 Bonn BBK-Zentrum-I@bbk.bund.de http://www.bbk.bund.de, Oficiul Federal de Poliţie Criminală (Bundeskriminalamt) 65173 Wiesbaden http://www.bka.de oder http://www.bundeskriminalamt.de

european de protecţie a infrastructurilor critice prin cel puţin trei modalităţi:

- adaptarea sistemului de legislaţie, de acţiune şi de reacţie în situaţii de urgenţă la cerinţele europene, în procesul pregătirii integrării şi integrării propriu-zise;
- dependenţele şi interdependenţele infrastructurilor vitale româneşti de cele europene;
- participarea la elaborarea şi punerea în aplicare a politicilor şi strategiilor de combatere a terorismului, traficului ilegal, crimei organizate şi ameninţărilor asimetrice.

Infrastructurile vitale româneşti sunt, aproape în totalitate, infrastructuri critice din cel puţin câteva motive esenţiale:

- provin din infrastructurile unei economii-gigant, inflexibile şi greu adaptabile economiei de piaţă, ale cărei urme nu au fost încă nici lichidate, nici ameliorate;
- economia şi societatea românească, în ansamblul ei, se află într-o stare de haos, specifică perioadelor îndelungi şi repetate de tranziţie, în care totul sau aproape totul este vital, critic şi vulnerabil;
- acţiunile fără discernământ asupra mediului, tăierea masivă a pădurilor, cultivarea haotică a terenurilor, dezastrul din agricultură, lipsa unei politici agrare, ecologice şi de protecţie a mediului coerente şi eficiente creează şi proliferează pericole extrem de grave la adresa tuturor infrastructurilor şi îndeosebi asupra celor critice;
- se aşteaptă ca participarea României la coaliţia antiteroristă şi la alte misiuni de gestionare a crizelor şi conflictelor şi de menţinere a păcii să genereze un nou tip de ameninţări asupra cetăţenilor şi infrastructurilor vitale ale economiei, societăţii, informaţiei şi condiţiilor de trai.

Desigur, pericolele şi ameninţările sunt mult mai numeroase. Ele fac obiectul unor iniţiative legislative, sunt cuprinse în strategia naţională de securitate şi în alte documente importante, dar sunt departe de a fi pe deplin monitorizate, gestionate, controlate şi înlăturate.

CONCLUZII ŞI PROPUNERI

1. Infrastructurile critice rămân un domeniu care se cere foarte bine investigat, monitorizat, analizat, evaluat, prognozat şi ameliorat.

2. Toate statele, Uniunea Europeană, în ansamblul ei, Statele Unite ale Americii şi alte ţări, alianţe, structuri de securitate internaţionale şi regionale îşi intensifică eforturile pentru a identifica, supraveghea, optimiza şi proteja infrastructurile vitale ale ţărilor, societăţilor, reţelelor şi ale lumii.

3. Considerăm că şi România, care se înscrie în acest amplu demers internaţional, trebuie să participe la acest proces, prin:

a) elaborarea unei strategii naţionale pentru PIC (în prezent, numai SUA au o astfel de strategie), în concordanţă cu recomandările europene şi internaţionale în domeniu;

b) inventarierea infrastructurilor critice pe domenii de activitate;

c) stabilirea vulnerabilităţilor specifice şi a modalităţilor de apărare;

d) elaborarea unor ghiduri sau seturi de norme privind PIC;

e) întărirea cooperării dintre sectorul public şi cel privat prin pachete de acte normative şi cointeresarea sectorului privat prin facilităţi fiscale, asistenţă de specialitate etc.

f) formarea unor echipe de specialişti pe diverse domenii, care să poată asigura expertiză de PIC;

g) introducerea în planurile de învăţământ şi cercetare din UNAp a unor teme specifice protecţiei infrastructurilor critice.

EDITURA UNIVERSITĂŢII NAŢIONALE DE APĂRARE „CAROL I“

Redactor: Corina VLADU
Tehnoredactor: Mirela ATANASIU

Bun de tipar: 31.07.2006
Hârtie: A3 Format: A5
Coli de tipar: 3 Coli editură: 1,5

Lucrarea conţine 48 de pagini
Tipografia Universităţii Naţionale de Apărare „Carol I“

CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE
Şoseaua Pandurilor, nr. 68-72, sector 5, Bucureşti
Telefon: (021) 319.56.49
Fax: (021) 319.55.93
E-mail: cssas@unap.ro
Adresă web: http://cssas.unap.ro

141/1287/06 C 317/2006